

KENT S. ROBINSON
Acting United States Attorney
District of Oregon

CHRISTOPHER L. CARDANI
Assistant United States Attorney
701 High Street
Eugene, OR 97401
Email: chris.cardani@usdoj.gov
Telephone: (541) 465-6771

CHARLES F. GORDER, JR., OSB #912874
Assistant United States Attorney
1000 S.W. Third Ave., Suite 600
Portland, OR 97204
Email: charles.gorder@usdoj.gov
Telephone: (503) 727-1000

Attorneys for United States of America

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

UNITED STATES OF AMERICA

CR 05-60008-02-HO

v.

PIROUZ SEDAGHATY,

Defendant.

**GOVERNMENT'S RESPONSE TO
DEFENDANT'S SUPPLEMENTAL
BASIS FOR SUPPRESSION OF
SEIZED COMPUTER INFORMATION**

I. STATEMENT OF FACTS

Both the United States of America and the Russian Federation have an interest in preventing the financing of terrorist activity and in stopping the provision of material support to terrorist organizations in all parts of the world, including in that part of the Russian Federation

called Chechnya. That mutual interest has been long-term. Conflict in the Caucasus region of the Russian Federation has waxed and waned since at least the mid-1990s. Indeed, as recently as last month, a suicide bombers killed eight policemen in two separate incidents in Chechnya.¹ The president of Russian Republic of Ingushetia which neighbors Chechnya was seriously injured in a bomb attack in June 2009. An Islamic terrorist group with roots in Chechnya claimed responsibility for that attack.²

As alleged in the indictment, in the year 2000 the Al Haramain organization which was headquartered in Saudi Arabia, and whose U.S. branch (Al Haramain USA) was then operated by defendant Sedaghaty in Ashland, Oregon, was involved in encouraging donations to support the so-called “mujahideen” fighting Russian forces in Chechnya. The conspiracy alleged in the indictment was formed for the purpose of covering up Al Haramain’s provision of “charitable” funds to the Chechen mujahideen.

In December 2008, representatives of the United States, including the prosecution team in this matter, met in Moscow with representatives of the Russian Federation, including the Russian Security Service often referred to as the “FSB,” to exchange information and evidence concerning the activities of Al Haramain in the Caucasus region of the Russian Federation. In defendant’s pleading entitled “Post-Hearing Additional Specification of Basis for Suppression Based on Dissemination of Information to Russian FSB and Request for Discovery”(CR 205),

¹ “Police killed by Chechen suicide bomber,” August 25, 2009, accessed at cnn.com on September 24, 2009.

² “Chechen militants claim responsibility for Siberia Dam Disaster,” August 21, 2009, accessed at www.france24.com on August 24, 2009.

defense counsel attempts to portray something sinister from this exchange of information concerning terrorism. Counsel alleges that such an exchange was an outrageous “quid pro quo” justifying the suppression of evidence obtained in the United States from Al Haramain USA’s computers. Since there is nothing “outrageous” about two nations which confront the threat of terrorism in exchanging useful information, and since the exchange of this information in 2008 has no logical relation to the seizure of the specific computer evidence pursuant to a warrant which the government intends to introduce at trial, the motion to suppress the computer evidence on this additional ground should be denied without further hearing or additional discovery.

**II. THE EXCHANGE OF INFORMATION CONCERNING
INTERNATIONAL TERRORISM BETWEEN THE
UNITED STATES AND RUSSIA IN THIS CASE**

The United States and the Russian Federation have a treaty which requires both countries to assist the other in providing evidence relevant to criminal prosecution. See Treaty Between the United States of America and the Russian Federation on Mutual Legal Assistance in Criminal Matters, June 17, 1999, S. Treaty Doc. No. 106-22 (2000). And beginning in 2000, at the direction of the Presidents of both the United States and the Russian Federation, officials from both countries formed a U.S.-Russia Counterterrorism Working Group (the “CTWG”) which was chaired by high officials from the Department of State and the Russian Foreign Ministry.³ The CTWG meet periodically to discuss counterterrorism topics of mutual interest to

³ Most recently, Presidents Obama and Medvedev renewed this arrangement by creating a Bilateral Presidential Commission with several working groups, including a “Foreign Policy and Fighting Terrorism Group” chaired by the U.S. Undersecretary of State and the Russian Deputy Foreign Minister. Fact Sheet: U.S.-Russia Bilateral Presidential Commission, released by the Office of the Press Secretary, The White House, July 6, 2009.

both countries. As part of this relationship, members of the law enforcement and intelligence community of both countries meet periodically as a sub-group.

The December 2008 meeting in Moscow with the FSB was the result of both a formal request under the Treaty by the United States Department of Justice for Russian assistance in this prosecution and informal discussion between FBI and FSB personnel as part of the intelligence-law enforcement sub-group of the CTWG.

At the December 2008 meeting, representatives of the Russian FSB provided the United States with certain evidence relevant to this prosecution as requested by the United States under the Treaty. For example, the Russian FSB disclosed that it had learned that Al Haramain had smuggled money into Chechnya through an Al Haramain office in Baku, Azerbaijan. Some of this money was funneled to the Kavkaz Islamic Institute, which was a training camp for the mujahideen in Chechnya. The money from this so-called charity was used “to purchase weapons, uniforms, medicine, communication devices, vehicles, and to pay religious extremists’ salaries.”

Similarly, according to the FSB, the Russian government intercepted a message from Aqeel Aqeel, who was both the head of Al Haramain in Saudi Arabia as well as the President of Al Haramain USA in Ashland, Oregon, to one Ibn Khattab, a Saudi citizen who was the head of the foreign mujahideen fighting the Russians in Chechnya. In the message, Aqeel Aqeel told the mujahideen leader:

The cargo is ready to be shipped: RPGs and rounds of ammunition for them, along with rounds for other systems; machine guns, Kalashnikov assault rifles, sniper rifles. We purchased 1000 rounds of ammunition, AGS,⁴ one PTUR “Fagot” [an anti-tank grenade launcher], 500 [bulletproof] vests.

⁴ AGS can refer to an “advanced gun system” or an “armored gun system.”

Pursuant to the Mutual Legal Assistance Treaty between the United States and Russia, the Russian government has confirmed that an FSB officer will be available to testify to this and other matters at the trial.

At the December 2008 meeting, U.S. law enforcement provided a copy of the computer hard drives lawfully seized from Al Haramain USA in Oregon pursuant to the warrant. Those hard drives contained substantial evidence of interest to the Russian government in its on-going efforts to counter terrorism in the Caucasus. For example, the Al Haramain USA hard drives contained the photographs of captured and dead Russian soldiers, as well as photographs of some of their identity papers. Knowing as we do the lengths our government will go to account for our POW/MIA soldiers fallen in combat, one can understand that Russia might have similar interest in examining the Al Haramain USA computers to account for its own soldiers.

During the period of time covered by the indictment, the preeminent English-language website dedicated to mujahideen propaganda was “Azzam.com.” Azzam.com also ran a website called “qoqaz.net” which was dedicated to supporting the jihad in Chechnya. The Al Haramain USA computer hard drives contained substantial evidence that Radmila Balobina, aka Sofia Balobina, aka Ptichka, who was one of defendant Sedaghaty’s so-called Islamic wives,⁵ was translating English material into Russian for a Russian-language version of qoqaz.net website.

For example, found in Al Haramain USA’s computers was an e-mail dated January 24, 2000, from an Al Haramain official in Saudi Arabia transmitting a post from the qoqaz.net

⁵ That is, a woman married to defendant Sedaghaty in an Islamic ceremony, but whose marriage was not registered civilly with the state. Ms. Balobina, who was originally from Azerbaijan and spoke Russian, was living with the defendant in Ashland at the time.

website entitled “Frequently Asked Questions about the Jihad in Chechnya.” See Exhibit “A.”

Included in this email was a so-called “Seven-Point Action Plan” encouraging Muslims to support the jihad in Chechnya. Al Haramain USA’s computers were used to translate this material into Russian for the qoqaz.net website. *See, e.g.*, Exhibit “B” which is from the Al Haramain USA computers and reflects the preliminary translation from English into Russian. In November 2000, Ms. Balobina was publicly “thanked” on the qoqaz.net website for her work on the Russian language version of the website.

Finally, the hard drives contained evidence of e-mail traffic sent out by Al Haramain officials in Saudi Arabia to a group list-serv called the “Sheeshaan” group. “Sheeshaan” is a transliteration of the Arabic word for Chechnya. Al Haramain distributed information about the jihad in Chechnya to the Sheeshaan group. Obviously, the Russian government would have an interest in learning about the details of these emails.

III. SHARING INFORMATION ABOUT INTERNATIONAL TERRORISM WITH A FOREIGN GOVERNMENT IS COMMENDABLE, NOT GROUNDS FOR SUPPRESSION

In his pleadings, defendant cites no case which holds that disclosure of information developed in a criminal investigation to a foreign government is misconduct at all, let alone the kind of “outrageous conduct” which justifies suppression of evidence. Indeed, none of the cases which counsel cite even deal with disclosure of information to foreign governments.

Since the events of September 11, 2001, there has been a paradigm shift in both policy and law about the sharing of information in an attempt to “connect the dots” to prevent future terrorist events. Federal officials have broad authority to share information, including foreign intelligence information obtained during criminal investigations such as the instant one, when

necessary to carry out their duties. Indeed, section 403-5d of Title 50 of the United States Code now reads as follows:

(D) Foreign Intelligence Information. --

(1) IN GENERAL. – Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401(a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person’s official duties subject to any limitations on the unauthorized disclosure of such information. . . . [I]t shall be lawful for information revealing a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local or foreign government official for the purpose of preventing or responding to such a threat. . . .

(2) DEFINITION – In this subsection, the term “foreign intelligence information” means –

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against –

- (i) actual or potential attack or other grave acts of a foreign power or an agent of a foreign power;
- (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
- (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to –

- (i) the national defense or security of the United States; or
- (ii) the conduct of the foreign affairs of the United States.

It requires little imagination to see how information in Al Haramain USA's computers concerning (1) killed and captured Russian soldiers, (2) how persons in the United States were encouraging and supporting so-called "mujahideen soldiers fighting jihad in Chechnya," and (3) the translation of such material into Russian was information with respect to a foreign power and territory that related to the conduct of foreign affairs of the United States and was relevant to the ability of the United States to prevent the threat of future international terrorism.

Defense counsel attempts to minimize the significance of this information because of its age. The computers were seized and imaged in 2004, only five years ago. As noted earlier, the Russian government to this very day is struggling with extremist activity in the Caucasus. Just as the United States would have an interest in five to ten-year old information concerning the recruitment of individuals by Al Qaida, certainly the Russian government would be interested in the recruitment and support of jihadists in Chechnya just five to ten years ago.

The defendant's citation to the rules of grand jury secrecy do not compel a contrary conclusion. First, the computer material seized pursuant to a Rule 41 criminal search warrant does not even implicate the rules of grand jury secrecy since the seizure was not "a matter occurring before the grand jury" for which an obligation of secrecy is imposed under Federal Rule of Criminal Procedure 6(e)(2)(B). But even if the rule of grand jury secrecy did apply,

///

Rule 6(e) has been amended to allow for disclosure to a foreign government official along the same lines as discussed above. See Fed. R. Crim. P. 6(e)(3)(A)(ii) and (D).

Far from being “outrageous,” cooperation between the United States and foreign government partners should be encouraged as a matter of public policy. Indeed, reliance upon the reports of the computer forensic officials of foreign government has been found to be the basis for establishing probable cause in an application for a search warrant. *United States v. Cartier*, 543 F.3d 442, 446-447 (10th Cir. 2008), *cert. denied*, 129 S. Ct. 1390 (2008). And the United States is a party to the Council of Europe’s Convention on Cybercrime.⁶ Article 23 of the Convention commits the parties to the Convention to cooperate:

to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Although the Russian Federation is not a party to this Convention, one can hardly argue that similar cooperation with a non-party state is the kind of “outrageous conduct” that would justify suppression of otherwise lawfully obtained evidence.

Furthermore, it was reasonable to provide the Russian government with copies of all of the Al Haramain USA hard drives rather than attempt to segregate out only portions of the drives for dissemination to the FSB. As the courts have noted “[g]iven the numerous ways information is stored on a computer . . . a search can be as much an art as a science.” *United States v. Brooks*, 427 F.3d 1246, 1252 (10th Cir. 2005). Indeed, in computer forensic analysis it is

⁶ Council of Europe, Convention on Cybercrime, ETS No. 185, Budapest, 23 November. 2001.

standard practice to provide an examiner with complete copies of a drive rather than bits and pieces of it. *See generally United States v. Hill*, 459 F3d 966, 974-75 (9th Cir. 2006) (discussion of technical issues concerning searching computers). Many of the files in the Al Haramain USA drives relevant to Chechnya had been deleted, and some were fragmented and had to be reassembled by forensic analysis. Many were in foreign languages, including Russian. The forensic tools used in Russia, as well as the focus of the Russians' analysis, could well be different than the tools used by our computer forensic expert in this case. Thus, it would be difficult for us to know "what parts of the hard drives" the Russians required in order for them to obtain useful intelligence from the Al Haramain USA drives to counter terrorism in Chechnya.

Finally, even if the Court considered the dissemination of this computer media with the Russian government to be somehow improper, there are no fruits of that dissemination to be suppressed at the upcoming trial. *Wong Sun v. United States*, 371 U.S. 471 (1963). The evidence from the Al Haramain USA hard drives comes from the independent forensic search of those computers by U.S. law enforcement officials, not from any search conducted by the Russians. Similarly, the evidence obtained by the United States from the Russian government which the government intends to introduce at the trial was obtained pursuant to a Mutual Legal Assistance Treaty request from the United States to Russia, not from whatever examination the Russian government may have subsequently conducted of the Al Haramain USA hard drives. Evidence obtained independent of some unconstitutional conduct cannot be suppressed. *See United States v Heckenkamp*, 482 F.3d 1142, 1148-49 (9th Cir.), *cert. denied*, 128 S. Ct. 635 (2007) (evidence seized from computer pursuant to warrant supported by independent evidence not suppressed). Consequently, the motion to suppress should be denied.

IV. CONCLUSION

For the reasons given above, the defendant's motion to suppress the evidence obtained from the Al Haramain USA computers should be denied without further hearing or additional discovery.

Dated this 25th day of September 2009.

KENT S. ROBINSON
Acting United States Attorney

/s/ Charles F. Gorder, Jr.
CHARLES F. GORDER, JR.
Assistant United States Attorney

/s/ Christopher L. Cardani
CHRISTOPHER L. CARDANI
Assistant United States Attorney